(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－124940
（P2002－124940A）
(43)公開日　平成14年４月26日(2002.4.26)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00		６０１Ｂ　５Ｊ１０４
12/46				６０１Ｅ　５Ｋ０３０
12/28			11/00	３１０Ｃ　５Ｋ０３３
12/18			11/18	
12/66			11/20	Ｂ

審査請求　未請求　請求項の数４　ＯＬ　（全 11 頁）　最終頁に続く

(21)出願番号　特願2000－315729(P2000－315729)

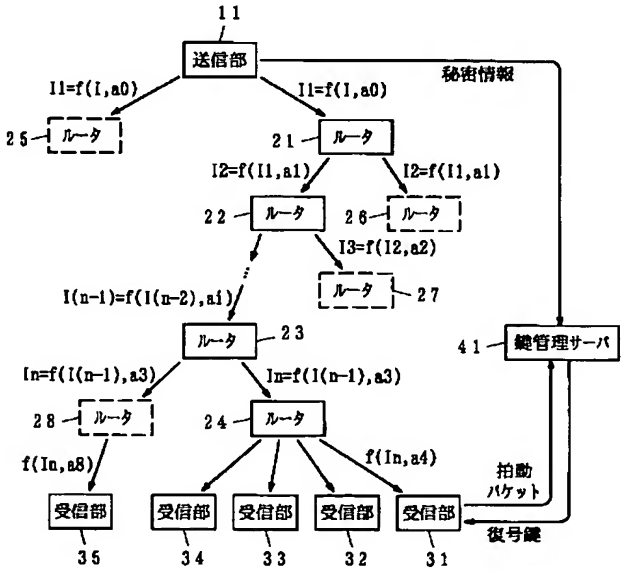
(22)出願日　平成12年10月16日(2000.10.16)

(71)出願人　000006297
村田機械株式会社
京都府京都市南区吉祥院南落合町３番地
(72)発明者　久保　博
京都市伏見区竹田向代町136番地　村田機械株式会社本社工場内
(74)代理人　100101948
弁理士　柳澤　正夫

Ｆターム(参考)　5J104 AA01 AA16 BA02 EA01 EA06
EA19 MA06 NA02 NA37 PA07
5K030 GA15 HC01 HD03 KA02 LD05
5K033 AA08 CB08 CB13 DB14 DB18
EC03

(54)【発明の名称】　マルチキャスト通信方法

(57)【要約】
【課題】　種々の不正行為が行われた場合でも、マルチキャスト通信全体の安全が脅かされないように保護したマルチキャスト通信方法を提供する。
【解決手段】　送信部１１は、暗号化に関する秘密情報を鍵管理サーバ４１に送出するとともに、暗号化に関する情報をルータ２１以降に伝達させる。まず、鍵要求情報ｈを暗号化して送出すると、ルータ２１～２４はそれぞれ固有の値ａｋを加算して順次送り、受信部３１～３４へ送信する。受信部は鍵要求情報を鍵管理サーバ４１に渡し、経路毎に異なる復号鍵Ｋを受け取る。配信される情報ｍは、所定の値ｙを用い、送信部１１でy^{a0}乗され、各ルータでも固有の値ａｋを用いてy^{ak}乗してｑの剰余を計算し、これを暗号として順次送る。これにより、経路毎に異なる暗号化が施される。受信部は、それぞれのルータで暗号化された情報を、取得した復号鍵Ｋにより１回の復号処理で復号し、平文ｍを取得する。



1

【特許請求の範囲】

【請求項１】　送信元から暗号化した情報を１以上の中継点を介して複数の受信先に配信するマルチキャスト通信方法であって、前記中継点では独立に生成した値ａを用いて前記送信元から与えられる所定値ｙをａ乗した値y^aを演算し、受け取った暗号化された情報をy^a乗し、その結果を前記送信元から与えられる値ｑで剰余演算して暗号化することを特徴とするマルチキャスト通信方法。

【請求項２】　前記送信元は、予め鍵要求情報を送出し、前記中継点は、前記鍵要求情報に前記値ａを加算して送出し、前記受信先は、受け取った鍵要求情報から復号鍵を取得して暗号化された情報を取得した前記復号鍵による一度の復号処理により平文を取得することを特徴とする請求項１に記載のマルチキャスト通信方法。

【請求項３】　受信先の少なくとも１つに情報を配信しないこととなったとき、該情報を配信しない受信先が接続されていた中継点の少なくとも１つは、前記独立に生成した値ａを変更して前記鍵要求情報を該中継点以降に配信することを特徴とする請求項２に記載のマルチキャスト通信方法。

【請求項４】　前記中継点は、経路変更によって前記鍵要求情報が変更されたとき、変更前後の鍵要求情報の差分に基づく暗号鍵を取得し、該暗号鍵により受け取った情報を暗号化してからy^a乗し、さらに剰余演算して暗号化することを特徴とする請求項１ないし請求項３のいずれか１項に記載のマルチキャスト通信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、送信元において暗号化した情報を複数の受信先に配信するマルチキャスト通信方法に関するものである。

【０００２】

【従来の技術】インターネット上での１対多や多対多の通信を行う為のＩＰマルチキャストが提案されたのは１９８８年のことである。マルチキャストの特徴は、インターネット上の多くの受信者に対して送信者が一度だけ情報の送信を行う点にある。送信された情報は経路上の中継点でコピーされ、次の各中継点あるいは各受信者に届けられる。そのため、１対１の通信技術（ユニキャスト）を使うと、例えば１００人の受信者に対して１００回同じ内容を送るのに比べて、送信者が送出するトラフィックは１／１００で済む。このため、送信者とネットワークの帯域を有効利用し、トラフィックの遅延を最小限にする通信技術として大きな期待が寄せられてきた。

【０００３】実際、１９９２年にはＭＢｏｎｅと呼ばれる実験的なＩＰマルチキャスト通信が始まっている。しかし同時期に開発されたＷＷＷとは対照的に、現在でもＩＰマルチキャストは広く利用されるに至っていない。この原因として、ＩＰマルチキャストの機能を盛り込んだルータが普及していないことが挙げられる。また、ＩＰマルチキャストが想定しているオーディオ、ビデオのリアルタイム配信などのアプリケーションを利用するのに十分な帯域を確保するには、まだ高額な費用がかかること、世界規模のルーティングに対応するルーティング技術の標準化がなかなか進まなかったことなども考えられる。

2

【０００４】しかし、最近これらの状況が変わりつつある。アメリカではＡＤＳＬなどによる家庭での常時接続が安価に提供されるようになってきており、インターネットラジオなどのマルチメディアアプリケーションが個人で楽しめるようになってきている。また、ＷＷＷのコンテンツを世界規模で高速に配信するコンテンツデリバリサービス会社がマルチキャストの応用を考えており、高速なマルチキャスト対応のバックボーンが整備されつつある。さらに、テレビ放送業界を巻き込んだ双方向デジタルテレビの標準化と実用化が急ピッチで進められている。これらの一連の動きによって、ＩＰマルチキャスト通信が普及する素地が整備されつつある。

【０００５】一方、マルチキャスト通信の商業利用の動きが進むにつれ、マルチキャスト通信でのセキュリティに関しても注目されるようになってきた。インターネットソサイエティ傘下にあって、インターネットの将来の発展に役立つ研究を推進している団体であるＩＲＴＦでも、安全なマルチキャスト通信に関する諸問題に取り組むためのＳＭｕＧという研究グループが発足し、課題の洗い出し、課題の解決方法について議論が進められている。また、タンパフリーなＩＣカードによるデジタルテレビ放送向けのセキュリティ製品を商品化する企業も現れてきた。

【０００６】しかし、ＩＰマルチキャストを一般に適用可能なスケーラビリティのある技術はまだ確立されていない。特に、暗号化された通信の復号鍵ばらまきによる海賊行為（ｐｉｒａｃｙ）に対抗する技術は、鍵所有者の追跡技術による抑止技術しか提案されておらず、ばらまかれた鍵での視聴を不可能にするような直接的な保護技術はほとんど存在しない。

【０００７】従来の暗号技術では、ただ一人でも全世界に向けて鍵のばらまきを行えば、そのマルチキャスト通信は世界中のどこででも不正に盗聴できる。すなわち、局所的な破れが即座に通信系全体の安全の崩壊につながることになる。このような状況に陥れば、被害の及ぶ範囲や被害額を見積もることすら困難であり、犯人が特定できても被った被害の補償ができるかどうか疑わしい。したがって、局所的に暗号系が破られたとしても、他の大部分の安全性を保護する仕組みがマルチキャスト通信の暗号系に組み込まれていることが望ましい。

【０００８】

【発明が解決しようとする課題】本発明は、上述した事情に鑑みてなされたもので、たとえ鍵がばらまかれた

り、あるいは平文と暗号文が公開された場合など、種々の不正行為が行われた場合でも、マルチキャスト通信全体の安全が脅かされないように保護したマルチキャスト通信方法を提供することを目的とするものである。

【０００９】

【課題を解決するための手段】本発明は、送信元から暗号化した情報を１以上の中継点を介して複数の受信先に配信するマルチキャスト通信方法であって、前記中継点では独立に生成した値ａを用いて前記送信元から与えられる所定値ｙをａ乗した値y^aを演算し、受け取った暗号化された情報をy^a乗し、その結果を前記送信元から与えられる値ｑで剰余演算して暗号化することを特徴とするものである。

【００１０】このように本発明では、マルチキャスト通信が通信パケットをバケツリレー式に伝送するという性質を利用し、中継点において独立に生成した値ａを用いた暗号化を行う。これによって、それぞれの配信経路により異なった暗号化が行われ、たとえ鍵がばらまかれても同一の配信経路以外での復号を行うことができない。また、本発明のように中継点で暗号化を行うことによって、平文と暗号文が公開されても、それらから復号鍵を生成することが困難である。従って、鍵がばらまかれたり、平文と暗号文が公開されるなどの不正行為が行われた場合でも、マルチキャスト通信全体の安全が脅かされることがない。

【００１１】また、送信元から予め鍵要求情報を送出し、中継点では、その鍵要求情報に値ａを加算して送出してゆく。このような操作を受けた鍵要求情報を受け取った受信先では、受け取った鍵要求情報から復号鍵を取得し、暗号化された情報を取得した復号鍵による一度の復号処理により平文を取得することができる。従って、中継点が多くなっても受信先においては手間を掛けずに平文を得ることができる。

【００１２】さらに、受信先の少なくとも１つに情報を配信しないこととなったときには、該情報を配信しない受信先が接続されていた中継点の少なくとも１つは、前記独立に生成した値ａを変更して前記鍵要求情報を該中継点以降に配信すればよい。これによって、配信しない受信先が現れても、鍵の変更を局所的に行えばよいため、影響を最小限に抑えることができる。

【００１３】さらにまた、経路変更によって前記鍵要求情報が変更されたとき、下流側の中継点において、変更前後の鍵要求情報の差分に基づく暗号鍵を取得し、該暗号鍵により受け取った情報を暗号化してからｙ^{a}乗し、さらに剰余演算して暗号化する。これによって、その中継点以降においては経路の変更前と同じ暗号鍵で暗号化し、また受信先においても同じ復号鍵で復号することができるので、鍵を変更する必要がない。

【００１４】

【発明の実施の形態】図１は、本発明のマルチキャスト通信方法の実施の一形態を実現する通信システムの一例を示すブロック図である。図中、１１は送信部、２１～２８はルータ、３１～３５は受信部、４１は鍵管理サーバである。以下の説明では、ルータを介して自律的なネットワークが相互に接続されたインターネット上のマルチキャスト通信のうち、特に放送型の通信について考える。しかしインターネットに限らず、情報が中継される各種の通信、例えば放送通信や、複数のＬＡＮを接続した閉じたネットワークシステムなどにおいても適用可能である。

【００１５】また、受信部３１～３５はインターネット上のさまざまな場所に存在するとし、マルチキャスト通信のトラフィックは、送信部１１からインターネットを「送信部１１にとって信頼できる」複数のルータを介してバケツリレー式に配信され、受信部まで届けられる。

【００１６】送信部１１は、例えば音声や動画といった番組のコンテンツなど、配信すべき情報を暗号化して配信する。また、正規の受信部においてそれぞれに到達するまでの経路に応じた復号鍵を生成するために、鍵要求情報を暗号化して配信する。なお、この鍵要求情報は一定時間ごとあるいは所定のタイミング毎に配信することとし、この鍵要求情報を含む暗号を以下の説明では拍動パケットと呼ぶことにする。

【００１７】図１に示すシステムでは、送信部１１から送出された暗号化された情報や拍動パケットは、１ないし複数のルータを経由して受信部３１～３５に配信される。例えば受信部３１～３４へは、ルータ２１，２２，…，２３，２４を経由して情報が配信される。また、受信部３５へは、ルータ２１，２２，…，２３，２８を経由して情報が配信される。ここでは少なくとも４つのルータを経由する例を示しているが、いくつのルータを経由するかは任意であるし、同じ数のルータを経由する場合でも、途中の経路が異なる場合もある。

【００１８】ルータ２１～２８は、送られてきた情報の配信先に応じて、次のルータあるいは受信部に対して、送られてきた情報を暗号化して転送する。例えばルータ２１は、送信部１１から送られてくる暗号化された情報をさらに暗号化して、ルータ２２，２６などに転送する。ルータ２２は、ルータ２１から送られてきた、ルータ２１で暗号化した情報に対してさらに暗号化し、ルータ２７や、ルータ２３に転送するための他のルータなどに転送する。後述するように各ルータ２１～２８は、暗号化の際に用いるパラメータをそれぞれ独立に任意に選択する。そのため、同じ情報を送っても、どのルータを経由するかによって、異なった暗号化の処理が施されることになる。このようにして、送信部１１から受信部３１～３５までの経路に応じた暗号化を実現することができる。なお、ルータ２１～２８は、「送信部１１にとって信頼できる」ものとする。「送信部１１にとって信頼できる」とは、送信部１１から知らされた秘密を他のノ

ードに漏らさない、ということである。

【００１９】図１では、暗号鍵ａを用いた暗号化処理をｆ（Ｉ，ａ）として示している。ここで、Ｉは受け取ったデータであり、暗号化された情報や拍動パケット等である。暗号化の処理ｆは、後述するように、暗号化された情報を暗号化する場合と拍動パケットを暗号化する場合とで異なる。暗号鍵ａは、それぞれのルータに固有のものである。なお、ここではルータ毎に暗号化の際に用いるパラメータを設定しているが、例えば送信する通信路毎に暗号化の際に用いるパラメータを設定してもよい。例えば最終段のルータ（ルータ２４など）が受信部に転送する際に通信路ごとに暗号化の際に用いるパラメータを設定すれば、各受信部毎に異なった暗号化処理を施すことが可能である。

【００２０】受信部３１～３５は、送信部１１及び経路上のルータによって暗号化された情報や拍動パケットを受け取る。拍動パケットを受け取ると、その拍動パケットを鍵管理サーバ４１に送り、復号鍵を受け取る。そして、鍵管理サーバ４１から受け取った復号鍵を用いて、１回の復号処理によって受信した暗号化された情報を復号し、情報の内容を取得することができる。

【００２１】この例では受信部３１～３４はルータ２４から同じ拍動パケット及び暗号化された情報を受け取る。もちろん上述のようにルータ２４が通信路毎に暗号化する場合には、異なる拍動パケット及び暗号化された情報を受け取ることになる。ここではこれらの受信部３１～３４が正規の受信者であるものとする。一方、受信部３５はルータ２８から拍動パケット及び暗号化された情報を受け取る。受信部３１～３４とは異なる経路を経由して受信するため、拍動パケット及び暗号化された情報は異なる暗号化処理を受けていることになる。

【００２２】鍵管理サーバ４１は、送信部１１から暗号化に関する秘密情報を受け取り、受信部３１～３５から送られてくる拍動パケットと秘密情報とから復号鍵を生成して、拍動パケットの送り元の受信部へ返信する。拍動パケットは各ルータにおいてそれぞれ暗号化処理が施されているので、送信部１１から送られる鍵要求情報を含んではいるが、経路によって異なった暗号化処理が施されている。そのため、経路途中でルータによって行われた暗号化処理も含めて復号できる復号鍵を生成することになる。後述するように、この復号鍵の生成は演算によって行うことができる。この鍵管理サーバ４１も、「送信部１１にとって信頼できる」ものとする。また、この鍵管理サーバ４１は、複数設けられていてよい。

【００２３】なお、鍵管理サーバ４１は、同じ拍動パケットに対しては同じ復号鍵を生成して返信するが、例えばばらまかれた拍動パケットに対応して復号鍵を受信部に返送しても、経路の異なる受信部では返送された復号鍵で情報を復号することはできない。また、鍵管理サーバ４１から取得した復号鍵がばらまかれても、経路の異なる受信部では、ばらまかれた復号鍵で情報を復号することはできない。

【００２４】このような構成によって、配信される情報は送信部１１で暗号化される。また、暗号化された情報は経路上の各ルータを通過するたびに、ルータ固有の暗号鍵によって暗号化される。これによって、インターネット上に分散した受信部には、送信部との経路に依存した別々の復号鍵を用いないと復号ができない。したがって、ルータをまたがった復号鍵のばらまきによる盗聴に対して安全性が保たれる。また、各ルータは自らの秘密を他のルータに漏らす必要がなく、また、どれか特定のルータの秘密が暴かれても、そのルータの直下以外では暗号が破られない。さらに、経路上のルータがいくつあっても、受信部で行う復号処理は１度だけでよい。すなわち、送信部１１からのホップ数によって復号処理は変わらないので、受信者間の公平性が保たれるという特徴を有している。

【００２５】次に、上述の構成における暗号化の手順を説明する。図２は、本発明の実施の一形態における送信部の動作を示すフローチャートである。まずＳ５１において、送信部１１及び鍵管理サーバ４１内の暗号器の初期化を行う。このとき、鍵管理サーバ４１は、復号鍵を生成する際に必要となる、暗号化に関する秘密情報を送信部１１から受け取る。なお、ルータ２１，２５に対しては、この時点で暗号化に必要となる情報を送信しておく。

【００２６】Ｓ５２において、送信部１１は情報の配信先へ宛てて、鍵要求情報を暗号化した拍動パケットを送出する。各ルータは、情報の配信先へのルーティングを開始すると同時に、独自の暗号鍵を生成し、また送信部１１から送出されている暗号化に必要となる情報を取得し、これらによって拍動パケットを暗号化して次のルータあるいは受信部へと送出する。

【００２７】このようにして経路が確立され、拍動パケットが配信された後、Ｓ５３において、実際に配信すべき情報を暗号化して送出する。この暗号化された情報も、各ルータを通過するごとにルータで暗号化され、次のルータあるいは受信部へ送出される。このとき、Ｓ５２で送出した拍動パケットと同じ暗号化のパラメータを用いて暗号化した情報の配信は、その拍動パケットと同じ経路を必ず経由するようにしなければならない。

【００２８】なお、Ｓ５２に示す拍動パケットの送出は、例えば所定時間毎や、所定のタイミング毎に行うことができる。また、その拍動パケットの送出ごとに、そのとき用いられた暗号化のパラメータを用いてＳ５３における情報の暗号化が行われることになる。もちろんＳ５１における暗号器の初期化についても、所定の時間経過や所定のタイミングにおいて実行してもよい。

【００２９】図３は、本発明の実施の一形態における受信部の動作を示すフローチャートである。配信されてき

た情報を受信部で受け取る際には、まずＳ６１において、直近のルータに対して、配信されている情報の受信を要求する。このとき、例えば鍵管理サーバ４１に対して加入の資格の有無などを確認する場合もある。

【００３０】受信要求が受理されると、直近のルータから拍動パケットを受け取る。受信部はＳ６２において、受け取った拍動パケットを鍵管理サーバ４１へ送出し、復号鍵を要求する。鍵管理サーバ４１は、受信部から受け取った拍動パケット（および送信部から予め送られてきている秘密情報）に従って、個々の受信部に個別の復号鍵を生成し、安全な方法で受信部に返送する。

【００３１】復号鍵を受け取った受信部は、Ｓ６３において、受け取った復号鍵を用い、配信されてくる暗号化された情報を復号し、情報の内容を取得することができる。なお、Ｓ６２における復号鍵の要求は、拍動パケットが配信されるたびに行い、そのとき受け取った復号鍵を用いて、拍動パケット配信後の暗号化された情報の復号を行う。

【００３２】以下、具体的な暗号化の手順について説明する。図４は、暗号化の方法の具体例の説明図である。この具体例では、所定値ｙをａ乗した値y^aを演算し、受け取った暗号化された情報をy^a乗し、そのべき乗結果を送信部１１では値ｐで、またルータでは値ｑで剰余演算することによって暗号化するものである。すなわち、情報をｍ、暗号をＣ、$Y=y^a$とすれば、

$C=m^Y$ （ｍｏｄ　ｐまたはｑ）　　（式１）

として求めるものである。ここで、所定値ｙ及び値ｑは、暗号化に必要となる情報として送信部１１から各ルータ２１～２８へ送出しておく。また、数ａは、送信部１１及び各ルータ２１～２８においてそれぞれ独立な固有の値でよい。例えばそれぞれ乱数などによって発生させてもよい。以下の説明では、送信部１１における数ａの値をａ０、ルータ２１～２８における数ａの値をａ１～ａ８とする。また、数ａ（ａ０～ａ８）は、それぞれ乱数によって生成するものとする。数ｑは大きな素数であり、この値は公開してかまわない。

【００３３】このような暗号化の処理を行う場合の動作について、図４とともに上述の図２，図３を用いながら説明してゆく。まずＳ５１における初期化の段階で、送信部１１は乱数ｈと大きな素数ｑ（ｑ＞２）を用意する。またｐ＝λ（ｑ）＝ｑ－１を用意する。ただし、λ（・）はＣａｒｍｉｃｈａｅｌ関数である。またｇｃｄ（ｐ，ｙ）＝１，１＜ｙ＜ｐを満たす適当な整数ｙを用意する。このようにして送信部１１の初期化を行った後、送信部１１はｐ，ｑ，ｙを直近のルータ（図１ではルータ２１，２５）に送信する。また、鍵管理サーバ４１に安全な方法でｈ，ｐ，ｑ，ｙを伝える。

【００３４】ここで、ｐは２と大きな素数との積になるようにすると、整数の集合$Z^*_p=\{y\in Z \mid gcd(p,y)=1,\ 1\leqq y<p\}$の元の個数が大きくなるので、ｙが推測されにくくなる。したがって、二つの整数ｑ’，２ｑ’＋１がともに素数となるようなｑ’を選び、ｐ＝２ｑ’，ｑ＝２ｑ’＋１とするとよい。

【００３５】このような準備ができたら、次に図２のＳ５２において、送信部１１は拍動パケットを送出する。送信部１１は、上述の乱数ｈ（ｈ∈Ｚ）を鍵要求情報ｈとし、ｈ０＝ｈ＋ａ０のように暗号化される。ここで鍵要求情報ｈは、文字列など、任意の情報でかまわないが、暗号化の際には整数値として見なして演算に供される。このようにして暗号化された鍵要求情報ｈ０（拍動パケット）がマルチキャストアドレスの宛先へ向けてネットワーク上に送出される。

【００３６】拍動パケットを受け取った各ルータでは、配信先へのルーティングを行うとともに、独自の数ａｋを生成する。例えばルータ２１は数ａ１を生成し、ルータ２２は数ａ２を生成する。また、送信部１１の直近のルータ以外のルータでは、直前のルータから数ｐ、ｑ、ｙも取得する。そして、送られてくる拍動パケットに対してａｋを加算して

ｈｋ＝ｈ（ｋ－１）＋ａｋ

の演算を行い、拍動パケットの暗号化を行う。すなわち、ルータ２１では

（ｈ＋ａ０）＋ａ１＝ｈ＋ａ０＋ａ１

を演算する。同様に、ルータ２２では、

（ｈ＋ａ０＋ａ１）＋ａ２＝ｈ＋ａ０＋ａ１＋ａ２

を演算することになる。従って、ルータ２１，２２，２３，．．．，２ｎを通過した拍動パケットは、受信部に到着した時には、

ｈｎ＝ｈ＋ａ０＋ａ１＋ａ２＋．．．＋ａｎ　　（式２）

となる。

【００３７】このようにして拍動パケットを送出した後、図２のＳ５３において、送信部１１は配信する情報を暗号化して送出する。このとき、送信部１１と各ルータは、予め

$y_k=y^{ak}$（ｍｏｄ　ｐ）　　（ｋ＝０，１，．．．，ｎ）

を計算して用意しておく。配信する情報をｍとするとき、送信部１１は、m^{y0}（ｍｏｄ　ｐ）を計算し、配信する情報の暗号として直近のルータ（ルータ２１，２５など）に送出する。ここで配信情報ｍも、文字列など、任意の情報でかまわないが、暗号化の際には整数値として見なして演算に供される。

【００３８】各ルータにおいては、上述の式１に従って暗号化処理を行う。すなわち、ルータ２１では

$(m^{y0})^{y1}$（ｍｏｄ　ｑ）$=m^{y0y1}$（ｍｏｄ　ｑ）$=m_1$

を演算する。同様に、ルータ２２では、

$(m^{y0y1})^{y2}$（ｍｏｄ　ｑ）$=m^{y0y1y2}$（ｍｏｄ　ｑ）$=m_2$

を演算することになる。従って、ルータ２１，２２，２３，．．．，２ｎを通過した配信する情報は、受信部に到着した時には、

$m^{y0y1y2...yn}$ （ｍｏｄ　ｑ）　　（式３）

となる。

【００３９】受信部（図４では受信部３１）では、何らかの方法でマルチキャスト通信のアドレスを発見し、ルータ（ルータ２ｎ）にマルチキャストアドレスの情報を要求する。この要求に応えて、ルータは上流のルータからｐ，ｑ，ｙを取得し、ａｎを生成した後、配信されている情報を受信部へ配送し始める。配送開始までの間に、受信者の認証などが行われる場合もある。

【００４０】ルータからの情報の配信が始まると、ま

$$y0 \cdot y1 \cdot \cdots \cdot yn \cdot d + k\lambda(q) = 1 \quad (式4)$$

を満たす（ｄ、ｋ）が求まれば、ｄが復号鍵になる。一方、

$$Y = y^{hn-h} (mod\ p) = y^{a0+a1+...+an} (mod\ p) \quad (式5)$$

とおくと、$Y \equiv y0 \cdot y1 \cdot \cdots \cdot yn \ (mod\ p)$であるから、ある整数$\mu$が存在して

$$Y = y0 \cdot y1 \cdot \cdots \cdot yn + \mu p \quad (式6)$$

が成り立つ。したがって、式５に従ってＹを求め、これを式４に代入すると、

$$(y - \mu p)\, d + k\lambda(q) = 1 \quad (式7)$$

となる。ここでｐ＝λ（ｑ）を代入し、ｋ’＝ｋ－μｄとして整理すると

$$Yd + k'\lambda(q) = 1 \ (= gcd(p, y)) \quad (式8)$$

となる。これを拡張ユークリッド互除法で解くと、（ｄ，ｋ’）が求まる。任意の整数ｋ’に対してｋ’＝ｋ－μｄを満たすｋは必ず存在するので、ここで求めたどのｄをとっても、復号鍵Ｋ＝ｄとできる。鍵管理サーバは、こうして求めた復号鍵Ｋを、受信部３１へ安全な方法で送信する。例えば公開鍵暗号を利用した鍵配送方法などを用いることができる。

【００４２】受信部３１は、鍵管理サーバ４１から受け取った復号鍵Ｋを用い、暗号化された情報ｍｎを復号する。受信した暗号化データｍｎ，鍵Ｋ，平文データｍの間には

$$mn^K = \{m^{y0y1...yn}\}^K$$
$$= m^{(1-k\lambda(q))}$$
$$\equiv m \ (mod\ q) \quad (式9)$$

の関係が成り立つ。したがって、受信部３１は受信した暗号化された情報ｍｎをZ^*_qの上でＫ乗することで復号し、もとの情報ｍを得ることができる。

【００４３】このようにして、情報の配信経路に応じた復号鍵を取得し、その復号鍵を用いて、配信されてきた暗号化された情報を復号し、情報の内容を取得することが可能になる。なお、この例では各ルータ毎に独立して数ａを生成して暗号化を行っているので、同じ経路を介して同じ最終段のルータから情報の配信を受ける受信部（例えば図１における受信部３１～３４）は同じ復号鍵を利用することになる。しかし異なる経路を介して情報を受け取る受信部（例えば図１における受信部３５）においては、拍動パケットや復号鍵が漏出しても、ルータ毎の暗号化の処理を復号できないため、情報の内容を取得することはできない。このように、経路が異なる受信部への復号鍵のばらまきに対して、安全性を保つことができる。

【００４４】ここで、一つ上流の拍動パケットを監視することによってｈ（ｎ－１）及びｈｎが取得でき、ａｎを容易に推定することができる。しかし、ｙは全ての受信者に対して秘密なので、y^{an}は分からない。したがって、上流のネットワークの鍵保有者および隣のネットワークの鍵保有者と結託しても復号鍵を作られることはない。また、下流のネットワークの鍵保有者と結託してもy^{-an}が分からないので同様に安全である。

【００４５】また、受信部においてはｑ，Ｋ，ｈ＋ａ０＋ａ１＋…＋ａｎを知ることになる。この条件から、悪意ある受信者が平文ｈを知ることができるか検討する。復号鍵Ｋから平文ｈを求めるには、ａ０＋ａ１＋…＋ａｎを求める必要がある。ところが復号鍵Ｋからａ０＋ａ１＋…＋ａｎを求めるには、受信者には秘密にされているｙを何らかの方法で手に入れた上で離散対数問題を解かなくてはならないので、非常に困難である。このため、復号鍵Ｋを持った受信者が平文ｈをばらまく攻撃を防ぐことができる。さらに、上述のように一つ上流の拍動パケットを監視することによりａｎは容易に推定されるが、ｙは受信者に対しては秘密なので、上流のネットワークの鍵保有者と結託しても復号鍵を作られることはない。

【００４６】さらにまた、別のネットワークの鍵保有者同士の結託した場合について考える。簡単のため、１，…，ｎ－１までは同一の経路を取り、ｎ段目のルータが別々の二つのネットワーク上の鍵保有者同士が結託する場合について考える。以下では、ｎ段目の二つのルータ

11

のパラメータを区別するのに右肩に括弧付きの添字を付ける。例えば、２つのｎ段目のルータの生成する乱数を

$$hn^{(1)} = h + a0 + a1 + \cdots + a(n-1) + an^{(1)} \quad (式10)$$

$$hn^{(2)} = h + a0 + a1 + \cdots + a(n-1) + an^{(2)} \quad (式11)$$

より、

$$hn^{(1,2)} = hn^{(1)} - hn^{(2)} = an^{(1)} - an^{(2)}$$

が求まる。またそれぞれの復号鍵を$K^{(1)}$、$K^{(2)}$とすると、

$$K^{(1)} = 1/(y0\,y1\cdots yn^{(1)} - \mu^{(1)}\ p) \pmod q \quad (式12)$$

$$K^{(2)} = 1/(y0\,y1\cdots yn^{(2)} - \mu^{(2)}\ p) \pmod q \quad (式13)$$

より、

$$K^{(2)}/K^{(1)} = (y0\,y1\cdots yn^{(1)} - \mu^{(1)}\ p)/(y0\,y1\cdots yn^{(2)} - \mu^{(2)}\ p) \pmod q \quad (式13)$$

である。しかし。$\mu^{(1)}$，$\mu^{(2)}$は未知であり、$hn^{(1,2)}$と連立させても、ｈやｙについて代数的に解くことはできない。したがって、別のネットワークの鍵保有者同士が結託しても、別のルーターの下にいる第三者の為の復号鍵は作られない。

【００４７】さらに、コンテンツをばらまかれた場合について考える。ネットワークをまたがってコンテンツが一部分でもばらまかれると、復号鍵を持たない受信者も暗号文と平文の組が手に入ることになる。この場合でも、暗号文ｍｎと平文ｍの組からｙ０ｙ１…ｙｎを求めることは離散対数問題になり難しい。復号鍵はｙ０ｙ１…ｙｎから求めるしかないので、結局、暗号文ｍｎと平文ｍから復号鍵Ｋを求めることは難しい。

【００４８】このように、本発明のマルチキャスト通信方法では、各種の不正が行われたとしても、マルチキャスト通信全体の安全が脅かされることはなく、安全に情報を配信することができる。

【００４９】上述の説明では、配信経路が特定されるものとして説明してきた。しかし、インターネット上の情報の転送経路は、ルータによって自律的かつ動的に変更される。上述のように本発明のマルチキャスト通信方法では、配信する情報の経路が変わると、経路に依存した暗号鍵も変わる。そこで、経路変更があっても受信者が継続してマルチキャストトラフィックを復号するには、経路変更と同時に鍵更新の作業が必要になる。しかし以下に説明するように、上述のような本発明のマルチキャスト通信方法では、配信経路が変更された場合においても、容易に対応することが可能である。

【００５０】図５は、配信経路の変更に対して受信部で対応する場合の説明図である。図中、７１は送信部、７２～７６はルータ、７７は受信部、７８は鍵管理サーバである。それぞれの機能は図１と同様である。図５では、ルータ７４，７６及び受信部７７が同じサブネットに接続されており、図５（Ａ）に示すようにルータ７４がマルチキャスト情報を配信しているとする。ここで、このサブネットへマルチキャスト情報を配信するルータがルータ７４から、図５（Ｂ）に示すようにルータ７６に変わる場合について、受信部７７で対応する例について説明する。

【００５１】まず、配信経路が変更されたことを検出しなければならない。ルータ７６は、当該サブネットへ情報を配信する前に、独立にａｎ’を生成し、拍動パケットｈ＋ａ０＋…＋ａｎ’を受信部７７に対して送出する。一方、受信部７７は、最近の拍動パケットｈ＋ａ０＋…＋ａｎを記憶しておき、拍動パケットを受けるたびにこれと比較することでルータの変更を検出することができる。

【００５２】次に、復号鍵を変更する。そのために、受信部７７は、新たに受け取ったｈ＋ａ０＋…＋ａｎ’を含む鍵要求パケットを鍵管理サーバ７８に送り、復号鍵Ｋ’を要求する。鍵管理サーバ７８は上述のような計算を行って、速やかにａ０＋…＋ａｎ’に対応した復号鍵Ｋ’を受信部７７に送り返す。このようにして受信部７７では、新たな配信経路に対応した復号鍵Ｋ’を入手し、ルータ７６から送られてくる暗号文ｍｎ’を復号して配信されてきたコンテンツを得ることができる。

【００５３】このように、配信経路を変更した場合には、その経路を利用していた受信部に対して新たな拍動パケットを送り、受信部で新たな復号鍵を取得することによって、それ以後も続けて情報の配信を受けることができる。

【００５４】図６は、配信経路の変更に対してルータで対応する場合の説明図である。図中、８１は送信部、８２～８７はルータ、８８は鍵管理サーバである。それぞれの機能は図１と同様である。図６では、ルータ８４，８６，８７が互いに接続され、図６（Ａ）に示すようにルータ８４がルータ８７へマルチキャスト情報を配信しているとする。ここで、ルータ８７へマルチキャスト情報を配信するルータが、ルータ８４から、図６（Ｂ）に示すようにルータ８６に変わる場合について説明する。

【００５５】まず、配信経路の変更を検出する。ルータ８６は、当該サブネットへ情報を配信する前に、ルータ８６に固有のａ’ｎ’を独立に生成し、拍動パケットｈ＋ａ０＋…＋ａ’ｎ’を送出する。一方、ルータ８７

は、最近の拍動パケットｈ＋ａ０＋･･･＋ａｎを記憶しておき、拍動パケットを受けるたびにこれと比較することでルータの変更を検出することができる。

【００５６】配信経路の変更を検出したルータ８７は、新たに受け取った拍動パケットを元に

ａ（ｎ，ｎ’）＝（ｈ＋ａ０＋…＋ａｎ）－（ｈ＋ａ０＋…＋ａ’ｎ’）

を計算し、鍵管理サーバ８８にａ（ｎ、ｎ’）とともに暗号鍵要求パケットを送出する。鍵管理サーバ８８は速やかに$y^{a(n,n')}$を暗号鍵として送り返す。これ以後、ルータ８７は$mn'^{y(a(n,n'))y(n+1)}$を下流に配信する。ここで、ｙ（ａ（ｎ，ｎ’））＝$y^{a(n,n')}$、ｙ（ｎ＋１）＝$y^{a(n+1)}$である。これによって、ルータ８７の下流では復号鍵の更新が不用になる。

【００５７】なぜなら、送信部８１からルータ８７に至るまでの経路上で、配信経路が変更された分岐点に当たるルータ８２がｊ番目のルータであるとすると、

ａ（ｎ，ｎ’）＝｛ｈｊ＋（ａ（ｊ＋１）＋…＋ａｎ）｝－｛ｈｊ＋（ａ’（ｊ＋１）＋…＋ａ’ｎ’）｝

＝（ａ（ｊ＋１）＋…＋ａｎ）－（ａ’（ｊ＋１）＋…＋ａ’ｎ’）

である。一方、

$mn'^{y(a(n,n'))}=(mj^{y'(j+1)'...y'n'})^{y(a(n,n'))}$

より、代入すると

$mn'^{y(a(n,n'))}=mj^{y(j+1)...yn}=mn$

である。従って、

$mn'^{y(a(n,n'))y(n+1)}=mn^{y(n+1)}=m(n+1)$

である。このように、ルータ８７の下流では、経路の切替後でも切替前と同じ復号鍵を用いて復号を行うことができる。そのため、受信部では配信経路の切替が発生しても、そのままで配信情報を受け取ることが可能である。

【００５８】マルチキャスト通信では、マルチキャストグループの会員が脱会すると、トラフィックの復号鍵を更新しなくてはいけない。これは、脱会者がそれ以降そのグループのマルチキャスト通信を傍受できないようにするためである。従来はマルチキャストグループの残りの全メンバーに対して更新されたグループ鍵をユニキャスト通信で配送する方法が提案されていた。しかし、この方法では、ネットワークの規模が大きくなるにつれ、鍵配送での受信者間の遅延とトラフィックが増大する。これに対して、上述の本発明のマルチキャスト通信方法を用いることによって、このような鍵更新を脱会したメンバーの所属するネットワークの直下に属する受信者に限定することができる。このため、更新された鍵配送の遅延とトラフィックの増大を軽減することができる。

【００５９】以下に局所的なグループ鍵更新の方法について、図１に示した構成を例にして説明する。ここではルータ２４の直下の受信部３４がマルチキャストグループから脱会したとする。ルータ２４は、固有の値ａｎにより暗号化を行っていたものとする。

【００６０】脱会があったことは、まず、鍵管理サーバ４１が知る。すると鍵管理サーバ４１は、ルータ２４に対して鍵更新要求を送る。これに対してルータ２４は固有の秘密の値ａｎをａ’ｎに更新する。更新したら、すぐに下流に新たな拍動パケットｈ（ｎ－１）＋ａ’ｎを送出する。

【００６１】脱会者以外のメンバー（受信部３１～３３）は、拍動パケットｈ＝ｈ（ｎ－１）＋ａ’ｎを受け取ると、暗号鍵に変更があったことを検知する。そして、鍵管理サーバ４１に対して拍動パケットｈ（ｎ－１）＋ａ’ｎを含む新たな復号鍵要求を送る。鍵管理サーバ４１は、すみやかに新たな復号鍵Ｋ’を計算して返す。

【００６２】ルータ２４は、新たな固有の値ａ’ｎを使ってマルチキャスト情報をｍ（ｎ－１）$^{y(a'n)}$のように暗号化して配信する。受信部３１～３３では、新たな復号鍵Ｋ’を用いて配信された情報を復号すればよい。なお、受信部３４は新たな拍動パケットを受け取れないか、あるいは受け取って新たな復号鍵を鍵管理サーバ４１に要求しても新たな復号鍵が発行されないので、以後、情報の配信を受けることができなくなる。

【００６３】この方法では、ルータ２４の直下で脱会があっても、マルチキャストトラフィック全体の鍵更新は不要である。また、この例では鍵の更新を行ったルータ２４の下流にはルータが存在しないが、もし存在する場合には、その下流のルータｎ＋１では、鍵更新を行ってもよいし行わなくてもよい。この場合、上述のルータにより経路変更を行う場合と同様の手順で暗号鍵更新を行えば、ルータｎ＋１の下流では鍵更新は不要である。また、ルータｎ＋１で暗号鍵を更新しなければ、その下流で上述のような復号鍵更新を行えばよい。

【００６４】以上のように、本発明のマルチキャスト通信方法を用いると、マルチキャストのグループ鍵管理がルータで区切られたセグメント毎に独立に行えるようになる。したがって、グループ全体にまたがった鍵管理が不用になり、広域にわたるグループ鍵配送問題を解決することができる。

【００６５】

【発明の効果】以上の説明から明らかなように、本発明によれば、経路上の各中継点で異なる鍵を用いて独立に暗号化するので、鍵のばらまきや平文と暗号文の公開などの不正行為による被害を局所に限定することができ、マルチキャスト通信全体の安全が脅かされることがないという、格別の効果を奏する。また受信先ではそれぞれの中継点による暗号化に対応した復号処理は必要なく、１回の復号処理により平文を取得することができる。さらに、メンバーの脱会による鍵更新を局所的に行えばよく、鍵更新に伴うトラフィック量を格段に減少させるこ

15　　16

とができる。さらにまた、配信経路の変更が発生した場合、中継点で容易に対応することができるとともに、その中継点より下流においては暗号鍵及び復号鍵を変更する必要がなく、受信先ではそのまま情報の受信を続けることができる。

【図面の簡単な説明】

【図１】本発明のマルチキャスト通信方法の実施の一形態を実現する通信システムの一例を示すブロック図である。

【図２】本発明の実施の一形態における送信部の動作を示すフローチャートである。

【図３】本発明の実施の一形態における受信部の動作を示すフローチャートである。

【図４】暗号化の方法の具体例の説明図である。

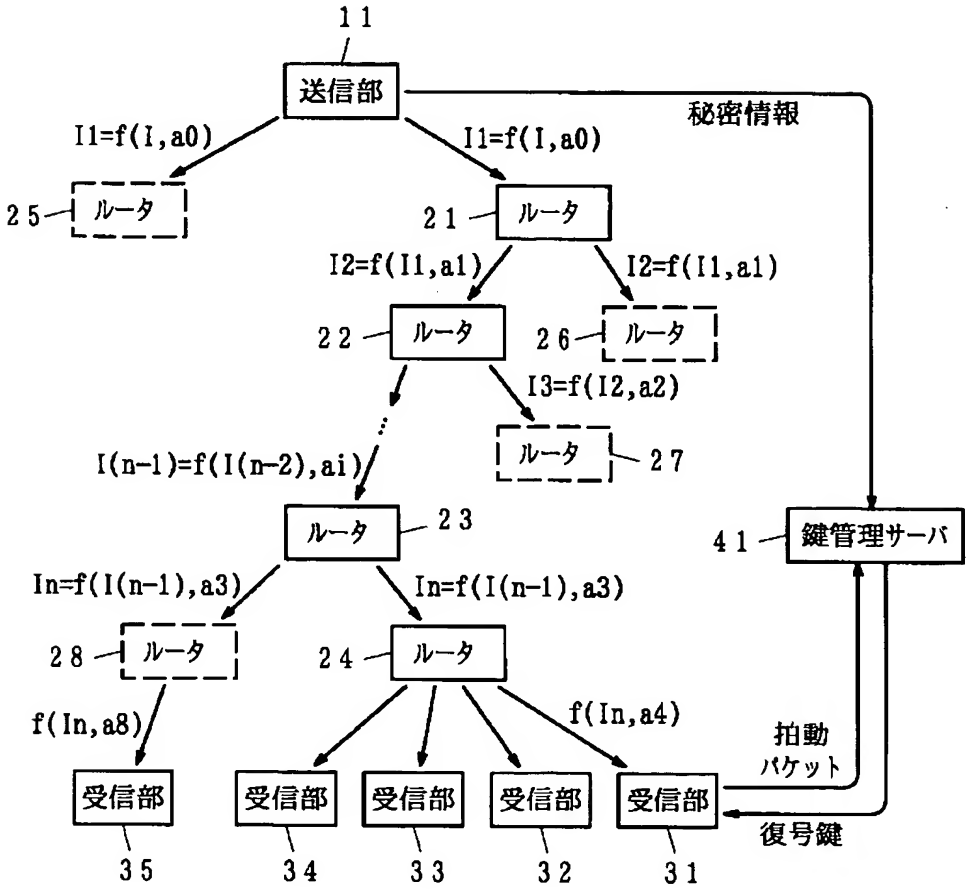
【図５】配信経路の変更に対して受信部で対応する場合の説明図である。

【図６】配信経路の変更に対してルータで対応する場合の説明図である。

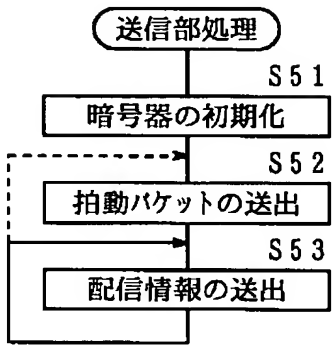
【符号の説明】

１１…送信部、２１～２８…ルータ、３１～３５…受信部、４１…鍵管理サーバ、７１…送信部、７２～７６…ルータ、７７…受信部、７８…鍵管理サーバ、８１…送信部、８２～８７…ルータ、８８…鍵管理サーバ。

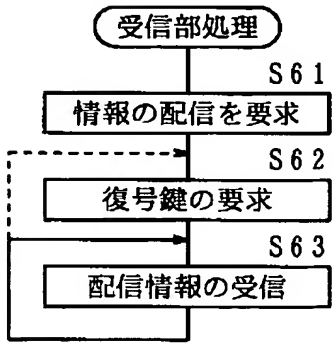
【図１】



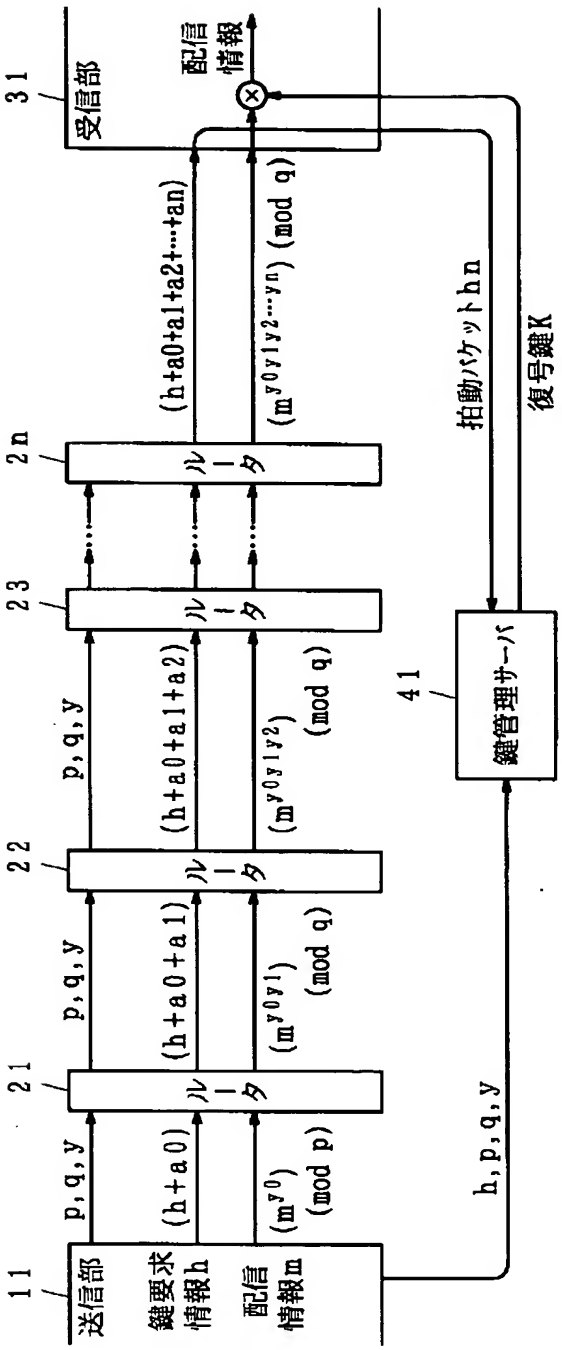
【図２】



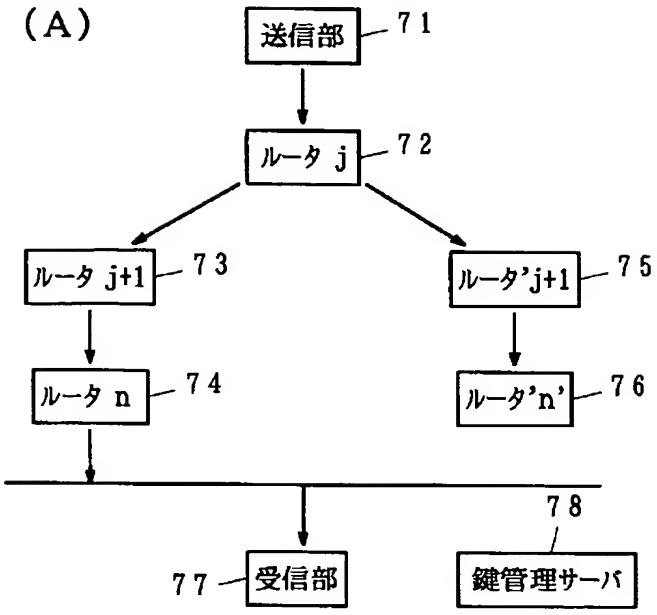
【図３】



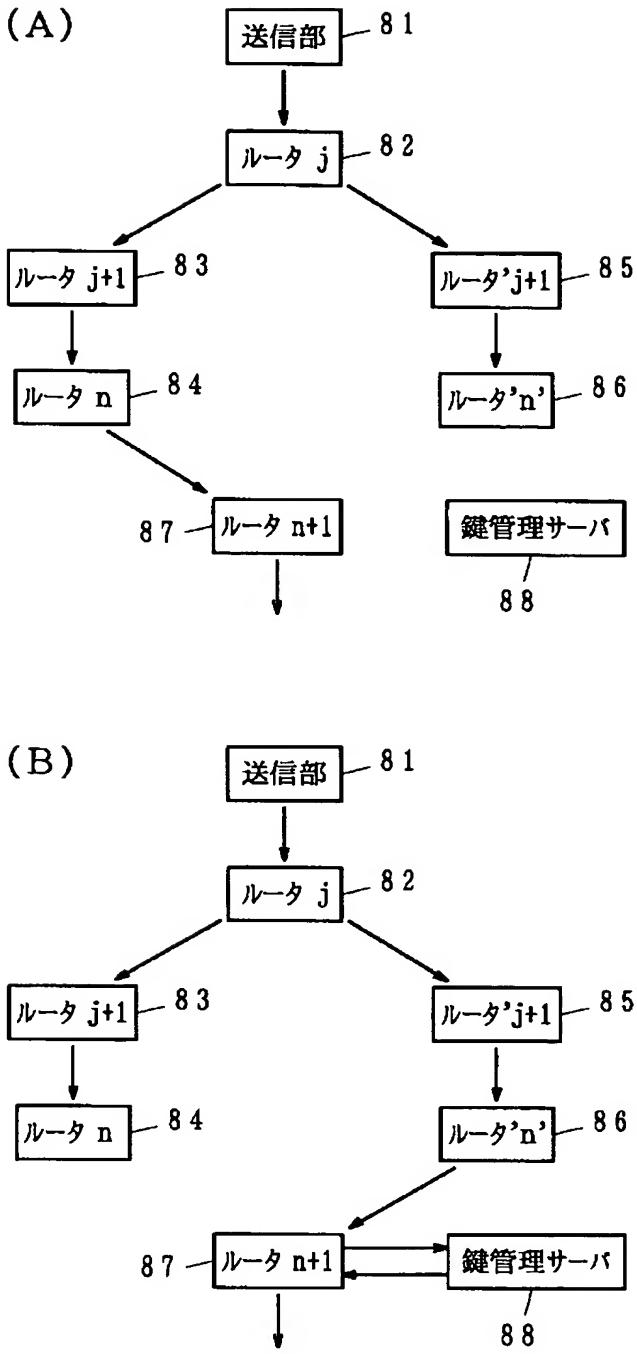
【図４】


11
送信部
鍵要求情報h
配信情報m
21
22
23
2n
ルータ
31
受信部
配信情報
41
鍵管理サーバ
p,q,y
(h+a0)
(m^y0) (mod p)
(h+a0+a1)
(m^y0y1) (mod q)
(h+a0+a1+a2)
(m^y0y1y2) (mod q)
(h+a0+a1+a2+…+an)
(m^y0y1y2…yn) (mod q)
h,p,q,y
拍動パケットhn
復号鍵K

【図５】



【図６】



フロントページの続き

(51)Int.Cl.[7]	識別記号	F I		テーマコード'(参考)
H04L 12/56		H04L 11/20	102A	
12/22		11/26		